Satoshi Hoshino
Filed 6/9/00
Q 59623
#2 1 of 6

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年　６月１０日

出 願 番 号
Application Number: 平成１１年特許願第１６４１７９号

出 願 人
Applicant (s): 甲府日本電気株式会社

２０００年　３月１７日

特許庁長官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号　出証特２０００－３０１７０７８

【書類名】　特許願
【整理番号】　03904964
【提出日】　平成11年 6月10日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 17/60
【発明者】
　【住所又は居所】　山梨県甲府市大津町１０８８－３　甲府日本電気株式会社内
　【氏名】　星野　聡
【特許出願人】
　【識別番号】　000168285
　【氏名又は名称】　甲府日本電気株式会社
【代理人】
　【識別番号】　100104916
　【弁理士】
　【氏名又は名称】　古溝　聡
【選任した代理人】
　【識別番号】　100095407
　【弁理士】
　【氏名又は名称】　木村　満
【手数料の表示】
　【予納台帳番号】　073679
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9901051
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子データ管理装置、方法及び記録媒体

【特許請求の範囲】

【請求項１】

電子データを入力するデータ入力手段と、

前記データ入力手段から入力された情報を記録する電子データ記録手段と、

着脱可能に構成された記録媒体が装着されたときに、該記録媒体が正当なものであるかどうかを認証する機器認証手段と、

特定人により操作されていることを認証する特定人認証手段と、

前記機器認証手段によって機器認証が得られ、且つ前記特定人認証手段によって特定人の認証が得られたときに、前記電子データ記録手段に記録されている電子データを修正するための修正データの入力を許可する修正許可手段と、

前記修正許可手段によって修正データの入力が許可されたときに、修正データを入力する修正データ入力手段と、

前記修正データ入力手段から入力された修正データに従って、前記電子データ記録手段に記録されている電子データを修正するデータ修正手段と、

前記データ入力手段からの電子データの入力の履歴と前記修正データ入力手段からの修正データの入力の履歴とを記憶管理する履歴管理手段と、

を備えることを特徴とする電子データ管理装置。

【請求項２】

前記履歴管理手段に記憶管理させるデータの入力の履歴を暗号化する手段をさらに備える

ことを特徴とする請求項１に記載の電子データ管理装置。

【請求項３】

前記機器認証手段によって機器認証が得られ、且つ前記特定人認証手段によって特定人の認証が得られたときに、前記履歴管理手段に記憶管理されているデータの入力の履歴を復号化する手段をさらに備え、

前記修正許可手段は、復号化されたデータの入力の履歴を出力し、外部に提示することによって前記電子データ記録手段に記録されている電子データの修正を

許可し、

前記修正データ入力手段は、該出力されたデータの入力の履歴に基づいて、修正データを入力する

ことを特徴とする請求項２に記載の電子データ管理装置。

【請求項４】

前記データ情報入力手段は、電子データを入力した者の認証情報を併せて入力するものであり、

前記修正データ入力手段は、修正データを入力した者の認証情報を併せて入力するものであり、

前記電子データ記録手段は、電子データまたは修正データを入力した者の認証情報を、入力された電子データまたは修正された電子データに対応付けて記録する

ことを特徴とする請求項１乃至３のいずれか１項に記載の電子データ管理装置。

【請求項５】

特定人の身体的特徴に関するデータを記憶する身体的特徴データ記憶手段をさらに備え、

前記特定人認証手段は、前記身体的特徴データ記憶手段に記憶されている身体的特徴に関するデータを操作する者の身体的特徴に関するデータと照合することによって特定人の認証を行う

ことを特徴とする請求項１乃至４のいずれか１項に記載の電子データ管理装置。

【請求項６】

前記記録媒体は、特定人の身体的特徴に関するデータを記録しており、

前記特定人認証手段は、さらに前記記録媒体に記録されている身体的特徴に関するデータを操作する者の身体的特徴に関するデータと照合することによって特定人の認証を行う

ことを特徴とする請求項５に記載の電子データ管理装置。

【請求項７】

前記電子データ記録手段には、前記データ入力手段から電子データの入力がある都度、入力された電子データが記録される

ことを特徴とする請求項１乃至６のいずれか１項に記載の電子データ管理装置。

【請求項８】

前記電子データ記録手段には、前記機器認証手段によって機器認証が得られ、且つ前記特定人認証手段によって特定人の認証が得られたときに、前記履歴管理手段に記憶されている電子データの入力の履歴に基づいて、入力された電子データが記録される

ことを特徴とする請求項１乃至６のいずれか１項に記載の電子データ管理装置。

【請求項９】

前記電子データ記録手段は、電子帳簿を記録するものであり、

前記電子データ及び前記修正データは、それぞれ電子帳簿に記録すべき取り引きに関する情報、該取り引きに関する情報を修正するための情報である

ことを特徴とする請求項１乃至８のいずれか１項に記載の電子データ管理装置。

【請求項１０】

電子データを記録する電子データ記録手段と、前記電子データ記録手段に記録される電子データの入力または修正の履歴を記憶管理する履歴管理手段とを備えるシステムにおける電子データ管理方法であって、

前記電子データ記録手段に記録するための電子データを入力するデータ入力ステップと、

前記データ入力ステップによる電子データの入力の履歴を前記履歴管理手段に記憶させる第１の履歴記憶ステップと、

前記データ入力ステップで入力された電子データを前記電子データ記録手段に記録させる電子データ記録ステップと、

着脱可能に構成された記録媒体が前記システムに装着されたときに、該記録媒体が正当なものであるかどうかを認証する機器認証ステップと、

特定人により操作されていることを認証する特定人認証ステップと、

前記機器認証ステップで機器認証が得られ、且つ前記特定人認証ステップで特定人の認証が得られたときに、前記電子データ記録手段に記録されている電子データを修正するための修正データの入力を許可する修正許可ステップと、

前記修正許可ステップで修正データの入力が許可されたときに、修正データを入力する修正データ入力ステップと、

前記修正データ入力ステップで入力された修正データに従って、前記電子データ記録手段に記録されている電子データを修正するデータ修正ステップと、

前記修正データ入力ステップによる修正データの入力の履歴を前記履歴管理手段に記憶させる第２の履歴管理ステップと、

を含むことを特徴とする電子データ管理方法。

【請求項１１】

前記データ情報入力ステップは、電子データを入力した者の認証情報を併せて入力するものであり、

前記修正データ入力ステップは、修正データを入力した者の認証情報を併せて入力するものであり、

前記電子データ記録ステップは、電子データを入力した者の認証情報を、入力された電子データに対応付けて前記電子データ記録手段に記録させ、

前記データ修正ステップは、修正データを入力した者の認証情報を、入力された修正データに従って修正された電子データに対応付けて前記電子データ記録手段に記録させる

ことを特徴とする請求項１０に記載の電子データ管理方法。

【請求項１２】

電子データを記録する電子データ記録手段と、前記電子データ記録手段に記録される電子データの入力または修正の履歴を記憶管理する履歴管理手段とを備えるシステムにおいて電子データを管理するためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記電子データ記録手段に記録するための電子データを入力するデータ入力ステップと、

前記データ入力ステップによる電子データの入力の履歴を前記履歴管理手段に記憶させる第１の履歴記憶ステップと、

前記データ入力ステップで入力された電子データを前記電子データ記録手段に記録させる電子データ記録ステップと、

着脱可能に構成された記録媒体が前記システムに装着されたときに、該記録媒体が正当なものであるかどうかを認証する機器認証ステップと、

特定人により操作されていることを認証する特定人認証ステップと、

前記機器認証ステップで機器認証が得られ、且つ前記特定人認証ステップで特定人の認証が得られたときに、前記電子データ記録手段に記録されている電子データを修正するための修正データの入力を許可する修正許可ステップと、

前記修正許可ステップで修正データの入力が許可されたときに、修正データを入力する修正データ入力ステップと、

前記修正データ入力ステップで入力された修正データに従って、前記電子データ記録手段に記録されている電子データを修正するデータ修正ステップと、

前記修正データ入力ステップによる修正データの入力の履歴を前記履歴管理手段に記憶させる第２の履歴管理ステップと、

を実行するためのプログラムを記録することを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項１３】

前記データ情報入力ステップは、電子データを入力した者の認証情報を併せて入力するものであり、

前記修正データ入力ステップは、修正データを入力した者の認証情報を併せて入力するものであり、

前記電子データ記録ステップは、電子データを入力した者の認証情報を、入力された電子データに対応付けて前記電子データ記録手段に記録させ、

前記データ修正ステップは、修正データを入力した者の認証情報を、入力された修正データに従って修正された電子データに対応付けて前記電子データ記録手段に記録させる

ことを特徴とする請求項１２に記載のコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、特に電子帳簿の管理に好適な電子データ管理装置、方法及びコンピュータ読み取り可能な記録媒体に関する。

【０００２】

【従来の技術】

取り引きに関する帳簿書類は、法律によって一定の期間保存することが義務づけられている。そして、平成１１年１月からデータを電子化した電子帳簿として、帳簿書類を保存することが認められるようになった。このような電子帳簿については、脱税、背任といった重大な犯罪行為を防止するために、通常の電子データに比べて不正アクセスに対する非常に高いセキュリティを達成することが要請されている。

【０００３】

【発明が解決しようとする課題】

これに対して、従来、一般的な電子データの管理方法として管理者の認証のために使用されているのは、パスワードである場合が多かった。パスワードによる認証では、パスワードが盗み出されてしまえば、誰でも管理対象としている電子データにアクセスすることができてしまう。このため、単純なパスワードでの認証による電子データの管理方法は、高度なセキュリティが要請される電子帳簿の管理に適用するのには適していなかった。

【０００４】

本発明は、上記従来技術の問題点を解消するためになされたものであり、電子帳簿などの電子データの管理について、高いセキュリティを達成することができる電子データ管理装置、方法及び電子データ管理のためのプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【０００５】

【課題を解決するための手段】

上記目的を達成するため、本発明の第１の観点にかかる電子データ管理装置は

電子データを入力するデータ入力手段と、

前記データ入力手段から入力された情報を記録する電子データ記録手段と、

着脱可能に構成された記録媒体が装着されたときに、該記録媒体が正当なものであるかどうかを認証する機器認証手段と、

特定人により操作されていることを認証する特定人認証手段と、

前記機器認証手段によって機器認証が得られ、且つ前記特定人認証手段によって特定人の認証が得られたときに、前記電子データ記録手段に記録されている電子データを修正するための修正データの入力を許可する修正許可手段と、

前記修正許可手段によって修正データの入力が許可されたときに、修正データを入力する修正データ入力手段と、

前記修正データ入力手段から入力された修正データに従って、前記電子データ記録手段に記録されている電子データを修正するデータ修正手段と、

前記データ入力手段からの電子データの入力の履歴と前記修正データ入力手段からの修正データの入力の履歴とを記憶管理する履歴管理手段と、

を備えることを特徴とする。

【０００６】

上記電子データ管理装置は、前記履歴管理手段に記憶管理させるデータの入力の履歴を暗号化する手段をさらに備えるものとしてもよい。

【０００７】

このような暗号化の手段を備える場合において、上記電子データ管理装置は、前記機器認証手段によって機器認証が得られ、且つ前記特定人認証手段によって特定人の認証が得られたときに、前記履歴管理手段に記憶管理されているデータの入力の履歴を復号化する手段をさらに備えるものとしてもよい。この場合、前記修正許可手段は、復号化されたデータの入力の履歴を出力し、外部に提示することによって前記電子データ記録手段に記録されている電子データの修正を許可し、前記修正データ入力手段は、該出力されたデータの入力の履歴に基づいて、修正データを入力するものとすることができる。

【０００８】

上記電子データ入力装置において、前記データ情報入力手段は、電子データを入力した者の認証情報を併せて入力するものとし、前記修正データ入力手段は、修正データを入力した者の認証情報を併せて入力するものとしてもよい。この場合、前記電子データ記録手段は、電子データまたは修正データを入力した者の認証情報を、入力された電子データまたは修正された電子データに対応付けて記録するものとすることができる。

【０００９】

上記電子データ管理装置は、また、特定人の身体的特徴に関するデータを記憶する身体的特徴データ記憶手段をさらに備えるものとしてもよい。この場合、前記特定人認証手段は、前記身体的特徴データ記憶手段に記憶されている身体的特徴に関するデータを操作する者の身体的特徴に関するデータと照合することによって特定人の認証を行うものとすることができる。

【００１０】

さらに、前記記録媒体が、特定人の身体的特徴に関するデータを記録していてもよい。この場合、前記特定人認証手段は、さらに前記記録媒体に記録されている身体的特徴に関するデータを操作する者の身体的特徴に関するデータと照合することによって特定人の認証を行うものとすることができる。

【００１１】

上記電子データ管理装置において、前記電子データ記録手段には、前記データ入力手段から電子データの入力がある都度、入力された電子データが記録されるものとすることができる。

【００１２】

また、前記電子データ記録手段には、前記機器認証手段によって機器認証が得られ、且つ前記特定人認証手段によって特定人の認証が得られたときに、前記履歴管理手段に記憶されている電子データの入力の履歴に基づいて、入力された電子データが記録されるものとすることもできる。

【００１３】

なお、上記電子データ管理装置において、前記電子データ記録手段は、電子帳簿を記録するものであることを好適とする。この場合には、前記電子データ及び

前記修正データは、それぞれ電子帳簿に記録すべき取り引きに関する情報、該取り引きに関する情報を修正するための情報とすることができる。

【００１４】

上記目的を達成するため、本発明の第２の観点にかかる電子データ管理方法は、

電子データを記録する電子データ記録手段と、前記電子データ記録手段に記録される電子データの入力または修正の履歴を記憶管理する履歴管理手段とを備えるシステムにおける電子データ管理方法であって、

前記電子データ記録手段に記録するための電子データを入力するデータ入力ステップと、

前記データ入力ステップによる電子データの入力の履歴を前記履歴管理手段に記憶させる第１の履歴記憶ステップと、

前記データ入力ステップで入力された電子データを前記電子データ記録手段に記録させる電子データ記録ステップと、

着脱可能に構成された記録媒体が前記システムに装着されたときに、該記録媒体が正当なものであるかどうかを認証する機器認証ステップと、

特定人により操作されていることを認証する特定人認証ステップと、

前記機器認証ステップで機器認証が得られ、且つ前記特定人認証ステップで特定人の認証が得られたときに、前記電子データ記録手段に記録されている電子データを修正するための修正データの入力を許可する修正許可ステップと、

前記修正許可ステップで修正データの入力が許可されたときに、修正データを入力する修正データ入力ステップと、

前記修正データ入力ステップで入力された修正データに従って、前記電子データ記録手段に記録されている電子データを修正するデータ修正ステップと、

前記修正データ入力ステップによる修正データの入力の履歴を前記履歴管理手段に記憶させる第２の履歴管理ステップと、

を含むことを特徴とする。

【００１５】

上記電子データ管理方法において、前記データ情報入力ステップは、電子デー

タを入力した者の認証情報を併せて入力するものとし、前記修正データ入力ステップは、修正データを入力した者の認証情報を併せて入力するものとしてもよい。この場合、前記電子データ記録ステップは、電子データを入力した者の認証情報を、入力された電子データに対応付けて前記電子データ記録手段に記録させるものとすることができ、前記データ修正ステップは、修正データを入力した者の認証情報を、入力された修正データに従って修正された電子データに対応付けて前記電子データ記録手段に記録させるものとすることができる。

【００１６】

上記目的を達成するため、本発明の第３の観点にかかるコンピュータ読み取り可能な記録媒体は、

電子データを記録する電子データ記録手段と、前記電子データ記録手段に記録される電子データの入力または修正の履歴を記憶管理する履歴管理手段とを備えるシステムにおいて電子データを管理するためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記電子データ記録手段に記録するための電子データを入力するデータ入力ステップと、

前記データ入力ステップによる電子データの入力の履歴を前記履歴管理手段に記憶させる第１の履歴記憶ステップと、

前記データ入力ステップで入力された電子データを前記電子データ記録手段に記録させる電子データ記録ステップと、

着脱可能に構成された記録媒体が前記システムに装着されたときに、該記録媒体が正当なものであるかどうかを認証する機器認証ステップと、

特定人により操作されていることを認証する特定人認証ステップと、

前記機器認証ステップで機器認証が得られ、且つ前記特定人認証ステップで特定人の認証が得られたときに、前記電子データ記録手段に記録されている電子データを修正するための修正データの入力を許可する修正許可ステップと、

前記修正許可ステップで修正データの入力が許可されたときに、修正データを入力する修正データ入力ステップと、

前記修正データ入力ステップで入力された修正データに従って、前記電子デー

タ記録手段に記録されている電子データを修正するデータ修正ステップと、

前記修正データ入力ステップによる修正データの入力の履歴を前記履歴管理手段に記憶させる第２の履歴管理ステップと、

を実行するためのプログラムを記録することを特徴とする。

【００１７】

上記コンピュータ読み取り可能な記録されたプログラムにおいて、前記データ情報入力ステップは、電子データを入力した者の認証情報を併せて入力するものとし、前記修正データ入力ステップは、修正データを入力した者の認証情報を併せて入力するものとしてもよい。この場合、前記電子データ記録ステップは、電子データを入力した者の認証情報を、入力された電子データに対応付けて前記電子データ記録手段に記録させるものとすることができ、前記データ修正ステップは、修正データを入力した者の認証情報を、入力された修正データに従って修正された電子データに対応付けて前記電子データ記録手段に記録させるものとすることができる。

【００１８】

【発明の実施の形態】

以下、添付図面を参照して、本発明の実施の形態について説明する。

【００１９】

図１は、この実施の形態にかかる電子帳簿管理システムの構成を示すブロック図である。図示するように、このシステムは、入力装置１８及び出力装置１９が接続された電子帳簿管理装置１と、これに着脱可能に構成された磁気カード２及びＩＣ（Integrated Circuit）カード４を備える。また、このシステムは、後述する管理者の身体的特徴としての指紋３のデータを取り込むようになっている。

【００２０】

磁気カード２は、このシステムのユーザ、すなわち取り引き情報の書き込みを行う者によって所有され、磁気カードリーダ１１へ挿入されたときにユーザによる取り引き情報の入力が可能となる。ＩＣカード４は、このシステムの管理者によって所有され、ＩＣカードリード／ライト１４へ挿入されたときに管理者による取り引き情報の修正、削除が可能となる。なお、ＩＣカード４には、管理者の

指紋のデータと所定の暗号鍵が予め記憶されている。

【００２１】

電子帳簿管理装置１は、専用のコンピュータ装置、またはカスタマイズされた汎用のコンピュータ装置によって構成され、ＣＰＵ（Central Processing Unit）１０ａを含む制御部１０と、磁気カードリーダ１１と、指紋認証装置１２と、指紋ファイル１３と、ＩＣカードリーダ／ライタ１４と、ＳＡＭ（Secure Application Module）１５と、電子帳簿ファイル１６と、履歴管理ファイル１７とを備えている。

【００２２】

制御部１０は、入力装置１８からの入力に従ってＣＰＵ１０ａが内部メモリ１０ｂに記憶されている後述するフローチャートに示すプログラムを実行することにより、磁気カードリーダ１１、指紋認証装置１２、ＩＣカードリーダ／ライタ１４及びＳＡＭ１５の動作を制御し、或いは電子帳簿ファイル１６及び履歴管理ファイル１７の内容を更新する。制御部１０は、また、所定の場合においてその処理結果を出力装置１９に出力する。なお、制御部１０は、履歴管理ファイル１７への履歴記録のためのタイマを有している。

【００２３】

磁気カードリーダ１１は、磁気カード２が挿入された場合に、当該磁気カード２に書き込まれているデータを読み出す。磁気カードリーダ１１は、読み出したデータにより、挿入された磁気カード２がユーザのものであるときには、その旨を制御部１０に通知する。

【００２４】

指紋認証装置１２は、指紋３を読み取るスキャナと、読み取った指紋３のデータを、指紋ファイル１３に記録されている指紋のデータ及びＩＣカード４から読み取られた指紋のデータとパターンマッチングする手段とを備える。指紋認証装置１２は、パターンマッチングによりすべての指紋のデータが一致したときに、読み取られた指紋３が管理者のものであると認証し、その結果を制御部１０に通知する。

【００２５】

指紋ファイル１３は、電子帳簿管理装置１内部の固定ディスク装置などに記憶され、予め指紋認証装置１２のスキャナから読み込まれた電子帳簿管理装置１の管理者（１人または複数人）の指紋３のデータを記録する。なお、指紋ファイル１３は、内容の改竄を防ぐために、ＩＣカードリーダ／ライタ１４に装着されたＩＣカード４が正当なものであるとの機器認証が得られた場合のみに、アクセス可能にしてもよい。

【００２６】

ＩＣカードリーダ／ライタ１４は、ＩＣカード４が挿入された場合に、当該ＩＣカード４に記録されているデータを読み出す。ＩＣカードリード／ライト１４は、ＳＡＭ１５との間で後述するような機器認証を行い、機器認証が得られたときにはその旨を制御部１０に通知する。なお、ＩＣカードリード／ライト１４は、ＩＣカード４へ指紋のデータ及び暗号鍵を書き込むために使用してもよい。

【００２７】

ＳＡＭ１５は、例えば、１チップの半導体装置によって構成され、暗号鍵（秘密鍵及び公開鍵）を格納している。ＳＡＭ１５及びＩＣカードリード／ライト１４は、ＩＣカードリード／ライト１４にＩＣカード４が挿入されたときに、内部に格納している暗号鍵とＩＣカード４に記録されている暗号鍵とによるチャレンジレスポンスの手法を用いて、機器認証を行う。

【００２８】

電子帳簿ファイル１６は、ＭＯ、ＣＤ－Ｒ、ＤＶＤなどの電子帳簿管理装置１から着脱可能に構成された読み書き可能な記録媒体に記憶され、図２に示すように、取引に関する情報とその情報を入力した者の電子署名とをそれぞれ対応付けて記録する。なお、電子帳簿ファイル１６へのデータの記録は、取り引きの発生の都度行われるか、或いは履歴管理ファイル１７に蓄積された情報に基づいて一括して行われる。

【００２９】

履歴管理ファイル１７は、電子帳簿管理装置１内部の固定ディスク装置などに記憶され、取引に関する情報及びその修正（削除を含む。以下、同じ）に関する情報を記録する。履歴管理ファイル１７に記録される情報は、図３に示すように

、日付、時間、利用者、利用内容、金額、正常終了フラグ、修正フラグ及び修正内容の各項目からなる。

【００３０】

履歴管理ファイル１７は、ユーザが入力した取り引きに関する情報の履歴、管理者が修正した取り引きに関する情報の履歴を、その入力、修正の都度記録していく。なお、履歴管理ファイル１７に記録されるデータは、すべてＳＡＭ１５に格納されている公開鍵によって暗号化されており、管理者が修正を行う場合にのみ、ＳＡＭ１５に格納されている秘密鍵で復号化される。

【００３１】

入力装置１８は、キーボードなどによって構成され、ユーザまたは管理者が取り引き情報を入力したり、処理を選択したりするために用いられる。出力装置１９は、ディスプレイ装置などによって構成され、制御部１０による処理結果のうちの所定のもの、例えば、管理者が電子帳簿ファイル１６を更新するときに復号化された履歴管理ファイル１７を出力する。

【００３２】

以下、この電子帳簿管理システムによる電子帳簿ファイル１６の管理方法について説明する。ここでは、取り引きの都度、電子帳簿ファイル１６へ取り引きに関する情報が書き込まれるものとする。また、このシステムでの電子帳簿ファイル１６の管理が開始する前に、管理者の指紋３のデータを指紋ファイル１３及び管理者が所有するＩＣカード４に予め書き込まれているものとする。

【００３３】

図４は、ユーザによる取り引き情報の入力の処理を示すフローチャートである。このフローチャートの処理は、ユーザによって磁気カード２が磁気カードリーダ１１に挿入され、その磁気カード２がユーザのものであることが制御部１０に通知されたときに開始する。

【００３４】

まず、ユーザは、入力装置１８から行った取り引きに関する情報と共に、当該ユーザの電子署名を入力する（ステップＳ１１）。すると、制御部１０は、内部タイマが示している日付、時刻、利用者名を入力された取り引きに関する情報及

び電子署名に付加する。さらに、制御部１０は、ＳＡＭ１５に格納されている公開鍵を取り出し、この公開鍵で取り引きに関する情報等を暗号化して、履歴管理ファイル１７へ記録する（ステップＳ１２）。

【００３５】

次に、制御部１０は、ステップＳ１１で入力された取り引きに関する情報及びユーザの電子署名を対応付けて、電子帳簿ファイル１６へ記録する（ステップＳ１６）。そして、このフローチャートの処理を終了する。

【００３６】

図５は、管理者による取り引き情報の修正の処理を示すフローチャートである。このフローチャートの処理は、管理者によってＩＣカード４がＩＣカードリード／ライト１４に挿入されたときに開始する。

【００３７】

まず、ＩＣカードリード／ライト１４及びＳＡＭ１５は、挿入されたＩＣカード４に格納されている暗号鍵とＳＡＭ１５に格納されている暗号鍵によるチャレンジレスポンスによって、挿入されたＩＣカード４が正当なものであるかどうかの機器認証を行う（ステップＳ２１）。そして、制御部１０は、ＩＣカードリード／ライト１４からの通知に従って、機器認証が得られたかどうかを判定する（ステップＳ２２）。

【００３８】

機器認証が得られたと判定した場合、制御部１０は、指紋認証装置１２に指紋３の照合を行わせる。この指紋の照合は、まず、指紋認証装置１２のスキャナで指紋３のデータを読み取り、これをＩＣカードリード／ライト１４でＩＣカード４から読み出した指紋のデータとパターンマッチングし、さらに、指紋ファイル１３に記録されている指紋のデータとパターンマッチングし、すべてが一致するかどうかを比較することによって行う（ステップＳ２３）。そして、制御部１０は、指紋認証装置１２からの通知に従って、指紋のデータが一致していたかどうかを判定する（ステップＳ２４）。

【００３９】

指紋のデータが一致していたと判定した場合、制御部１０は、ＳＡＭ１５に格

納されている秘密鍵を取り出し、この秘密鍵を用いて履歴管理ファイル１７に格納されているデータを復号化する。そして、制御部１０は、復号化した履歴管理ファイル１７の内容を出力装置１９に出力する（ステップＳ２５）。次に、管理者は、出力装置１９から出力された履歴管理ファイル１７のデータに従って、修正後のデータを、当該管理者の電子署名と共に入力装置１８から入力する（ステップＳ２６）。

【００４０】

制御部１０は、内部タイマが示している日付、時刻、利用者名を入力された修正後のデータ及び電子署名に付加する。さらに、制御部１０は、ＳＡＭ１５に格納されている公開鍵を取り出し、この公開鍵で修正後のデータ等を暗号化して、履歴管理ファイル１７へ記録する（ステップＳ２７）。次に、制御部１０は、ステップＳ２７で入力された修正後のデータに従って、電子帳簿ファイル１６に記録されているデータを更新し、それと共に入力された電子署名を記録させる（ステップＳ２８）。そして、このフローチャートの処理を終了する。

【００４１】

一方、ステップＳ２２で機器認証が得られなかったと判定された場合、及びステップＳ２４で指紋３のデータが一致しなかったと判定された場合には、そのままこのフローチャートの処理を終了する。

【００４２】

以下、この実施の形態にかかる電子帳簿管理システムで行っているセキュリティ達成のための手段について、（１）～（４）に列記して分かり易く示す。

【００４３】

（１）電子帳簿ファイル１６へ記録されているデータを修正するためには、ＩＣカード４による機器認証と、指紋３による管理者の本人認証との双方が得られなければならない。このため、単純なパスワードによる認証等に比べると、システムの管理者以外の者が電子帳簿ファイル１６へ記録されているデータを修正することができるようになる可能性が、非常に低くなる。

【００４４】

（２）管理者の指紋３のデータのパターンマッチングを、指紋ファイル１３に登

録されている指紋のデータとＩＣカード４に記録されている指紋のデータとの両方で行っている。このため、指紋ファイル１３に記録されているデータが改竄されたり、ＩＣカード４が偽造されたれたりしただけで、その両方がされない限り、電子帳簿ファイル１７に記録されている情報を修正することができない。

【００４５】

（３）電子帳簿ファイル１６へ記録している取り引きに関する情報には、それぞれ入力または修正を行ったものの電子署名が付されている。このため、誰が電子帳簿ファイル１６に記録されている取り引きに関する情報の入力を行ったか、或いは修正を行ったかが一目瞭然となり、電子帳簿ファイル１６に記録されているデータの正当性が確保される。

【００４６】

（４）履歴管理ファイル１７へ取り引きに関する情報の入力、修正の履歴を記録する場合には、ＳＡＭ１５に格納されている公開鍵を利用して暗号化を行っている。そして、履歴管理ファイル１７に記録されている履歴が復号化されるのは、ＩＣカード４の機器認証、指紋３の認証の双方が得られた場合だけである。このため、システムの管理者以外の者によって履歴管理ファイル１７に記録されているデータが不正に読み出されてしまうことがない。

【００４７】

すなわち、この実施の形態にかかる電子帳簿管理システムでは、予め登録した管理者以外の者が電子帳簿ファイル１６にアクセスできる可能性が極端に低くなり、電子帳簿ファイル１６の管理に対して高度なセキュリティを達成することが可能となる。また、履歴管理ファイル１７の記録内容を読み出すことも難しくなり、高度なセキュリティを達成することができる。

【００４８】

本発明は、上記の実施の形態に限られず、種々の変形、応用が可能である。以下、本発明に適用可能な上記の実施の形態の変形態様について、説明する。

【００４９】

上記の実施の形態では、管理者を認証するための身体的特徴として、指紋３によるものとしていた。しかしながら、管理者という認証を得るための身体的特徴

としては、指紋３以外の他の身体的特徴、例えば、虹彩、手形、顔、声、網膜などのを適用することもできる。また、ＩＣカード４による機器認証と共に、このような身体的特徴に加えて、或いはこれに代えて、パスワードによって管理者本人を認証するものとしてもよい。

【００５０】

上記の実施の形態では、電子帳簿管理システムの動作例として、取り引きに関する情報が入力される都度、その情報が電子帳簿ファイル１６へ記録される者としていた。しかしながら、電子帳簿ファイル１６への記録は、管理者のみが行えるものとしてもよい。この場合、図４のフローチャートの処理は、ステップＳ１３がなくなり、ステップＳ１２の処理で終了することとなる。

【００５１】

また、このような場合において管理者がＩＣカード４をＩＣカードリード／ライト１４に挿入したときに実行される処理を、図６のフローチャートに示す。最初に図５のステップＳ２１～Ｓ２４の処理が行われる（ステップＳ３１）。次に、管理者は、入力装置１８を操作することによって、取り引きに関する情報の修正か、新たな記録かのいずれかの処理を選択する（ステップＳ３２）。制御部１０は、選択された処理が取り引きに関する情報の修正か、それとも記録であるかを判定する（ステップＳ３３）。

【００５２】

選択された処理が修正であった場合には、図５のステップＳ２５～Ｓ２８の処理が行われ（ステップＳ３４）、このフローチャートの処理を終了する。選択された処理が記録であった場合には、制御部１０は、ＳＡＭ１５に格納されている秘密鍵を取り出し、履歴管理ファイル１７に記録されているデータを復号化する。そして、制御部１０は、復号化したデータのうちでまだ電子帳簿ファイル１６に記録されていないものを電子帳簿ファイル１６に記録する（ステップＳ３５）。そして、このフローチャートの処理を終了する。

【００５３】

上記した図６のフローチャートに示す処理によることで、電子帳簿ファイル１６に取り引きに関する情報を記録する場合には、管理者が必ず介在することにな

る。このため、この変形例での管理方法によることで、上記の実施の形態の管理方法よりも、電子帳簿ファイル１６へのアクセスに対してさらに高度なセキュリティを達成することができるようになる。

【００５４】

上記の実施の形態では、電子帳簿ファイル１６及びその履歴管理ファイル１７の管理に本発明を適用した場合を例として説明した。しかしながら、本発明は、電子帳簿以外の電子データ、特に電子帳簿と同程度にデータの盗用や改竄からの保護の要請が高い電子データの管理について、適用することができる。

【００５５】

上記の実施の形態では、図４、図５のフローチャートに示すプログラム（または、変形例で示した図６のフローチャートに示すプログラム）は、制御部１０の内部メモリ１０ｂに記憶されているものとし、ＣＰＵ１０ａがこれを実行するものとしていた。

【００５６】

しかしながら、このようなプログラムは、図７（ａ）に示すように、コンピュータ読み取り可能な記録媒体として、例えばＭＯ５１に格納し、ＭＯドライブ５０で読み取って制御部１０の内部メモリ１０ｂに記憶させるものとしてもよい。或いは、図７（ｂ）に示すように、このようなプログラムをサーバ６２に蓄積させておき、通信装置６０からネットワーク６１を介してサーバ６２に要求を行い、サーバ６２に蓄積されているプログラムを搬送波に重畳させたプログラムデータ信号をネットワーク６１を介して通信装置６０が受け取り、制御部１０の内部メモリ１０ｂに記憶させるものとしてもよい。なお、図７（ａ）、（ｂ）において図示しない他の構成は、図１に示すものと同じである。

【００５７】

【発明の効果】

以上説明したように、本発明によれば、電子帳簿などの電子データの管理について、高度なセキュリティを達成することができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態にかかる電子帳簿管理システムの構成を示すブロック図である。

【図２】

図１の電子帳簿ファイルに記録されるデータを示す図である。

【図３】

図１の履歴管理ファイルに記録されるデータを示す図である。

【図４】

ユーザが取り引き情報を入力するときの処理を示すフローチャートである。

【図５】

管理者が取り引き情報を変更するときの処理を示すフローチャートである。

【図６】

電子帳簿ファイルへの記録がすべて管理者によって行われる場合の処理を示すフローチャートである。

【図７】

（ａ）、（ｂ）は、本発明の実施の形態の変形例にかかる電子帳簿管理システムの簡略化した構成を示すブロック図である。

【符号の説明】

１　電子帳簿管理装置

２　磁気カード

３　指紋

４　ＩＣカード

１０　制御部

１０ａ　ＣＰＵ

１０ｂ　内部メモリ

１１　磁気カードリーダ

１２　指紋認証装置

１３　指紋ファイル

１４　ＩＣカードリーダ／ライタ

１５　ＳＡＭ

１６　電子帳簿ファイル

１７　履歴管理ファイル

１８　入力装置

１９　出力装置

５０　ＭＯドライブ

５１　ＭＯ

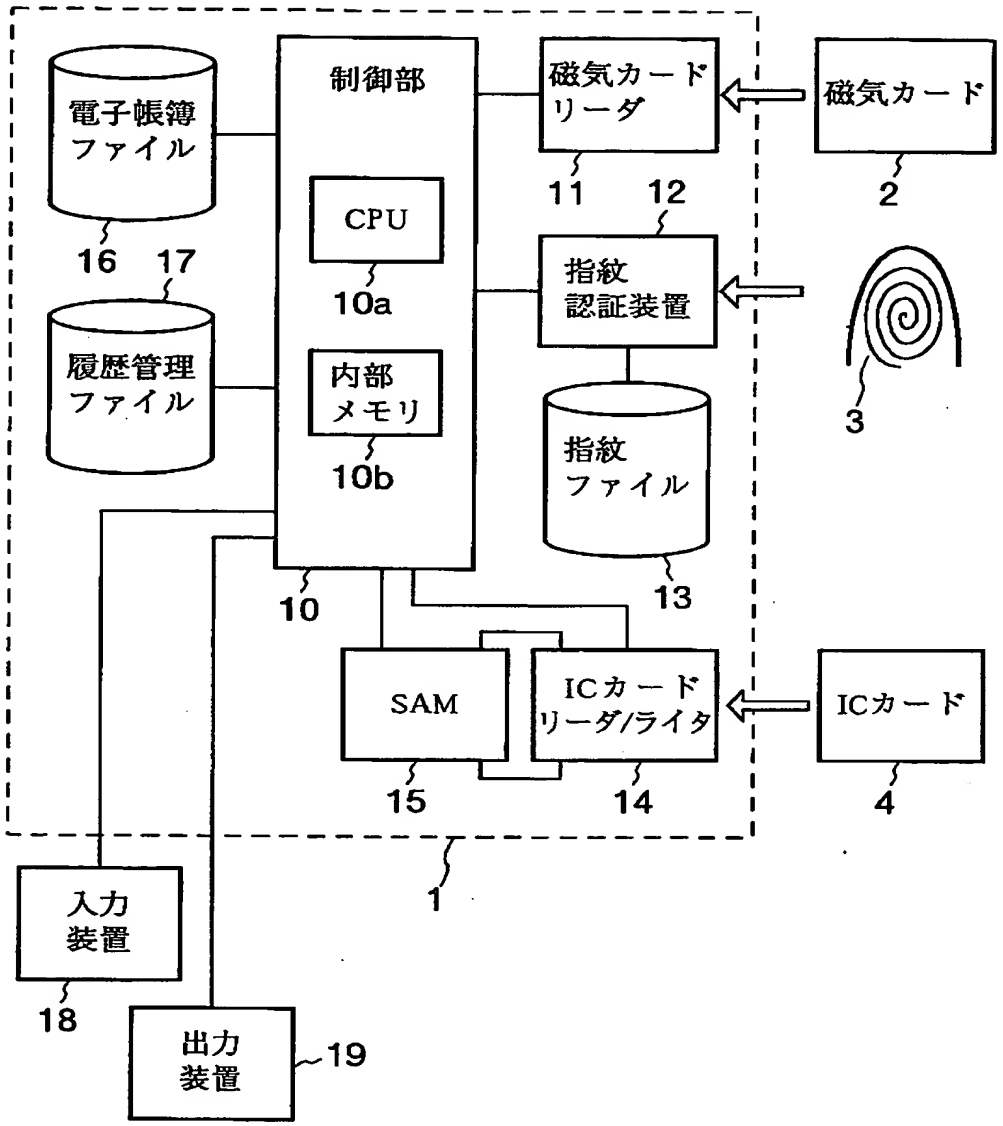
６０　通信装置

６１　ネットワーク

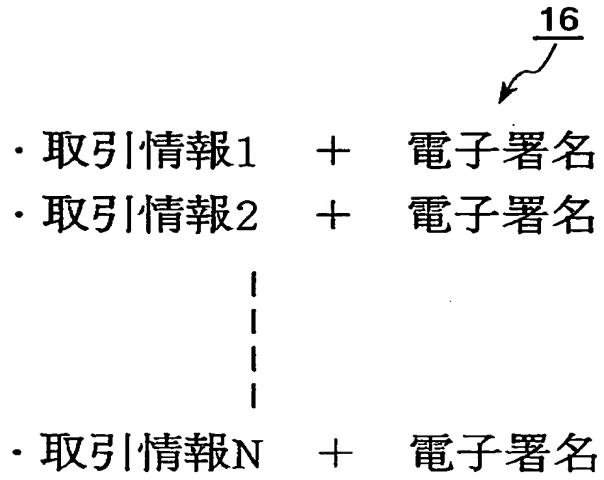
６２　サーバ

【書類名】　図面

【図１】


制御部
電子帳簿
ファイル
16
17
履歴管理
ファイル
CPU
10a
内部
メモリ
10b
10
磁気カード
リーダ
11
12
磁気カード
2
指紋
認証装置
3
指紋
ファイル
13
SAM
15
ICカード
リーダ/ライタ
14
ICカード
4
1
入力
装置
18
出力
装置
19

【図２】

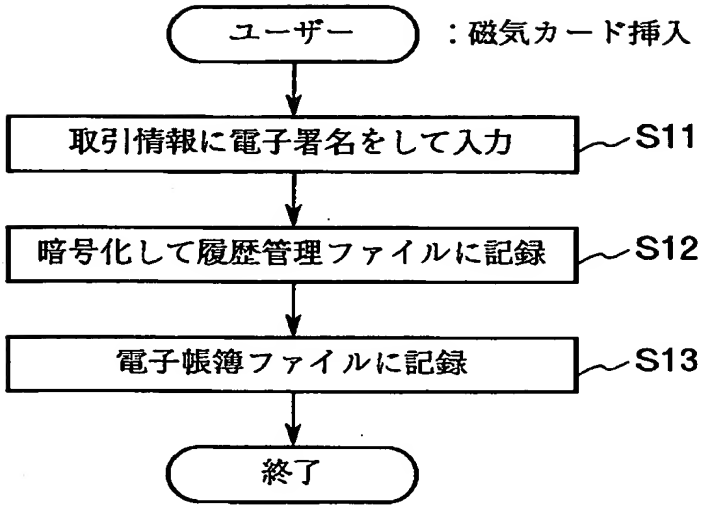


【図３】

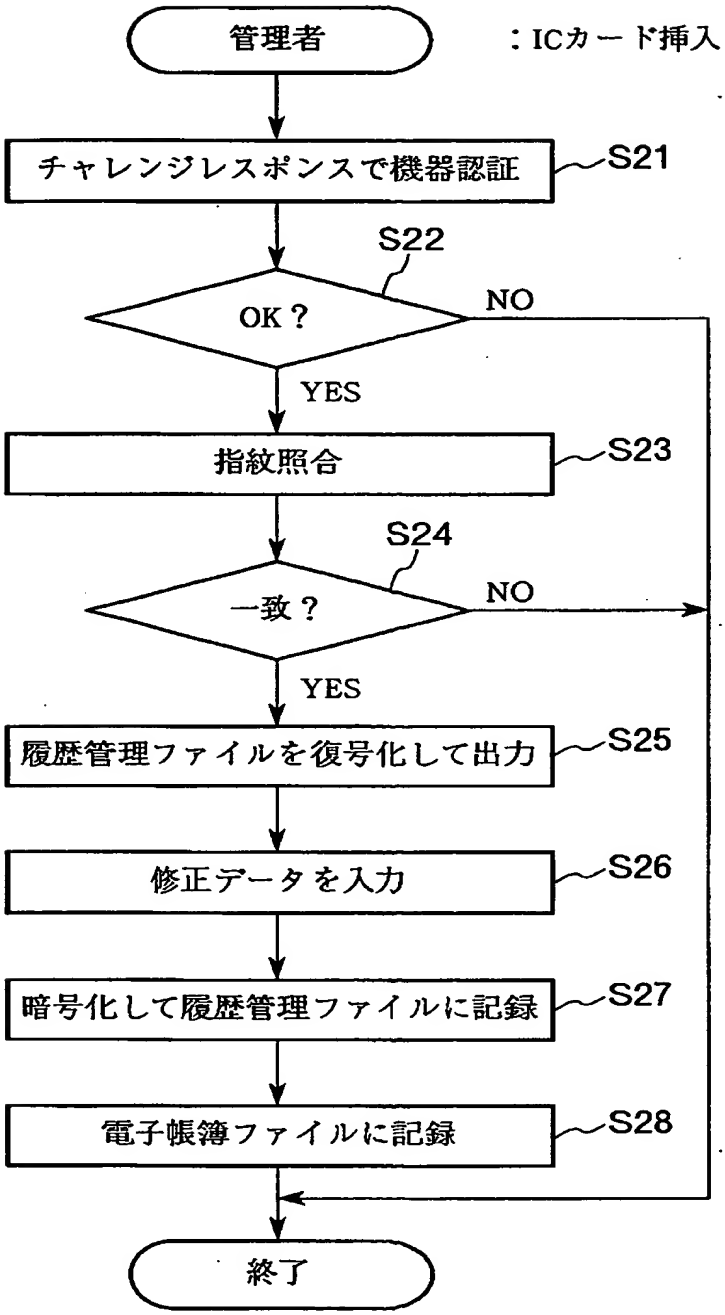
17

日付	時間	利用者	利用内容	金額	正常終了？	修正？	修正内容
○月○日	XX:XX	①△△△	出金	10,000	○(電子署名)	無	—
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

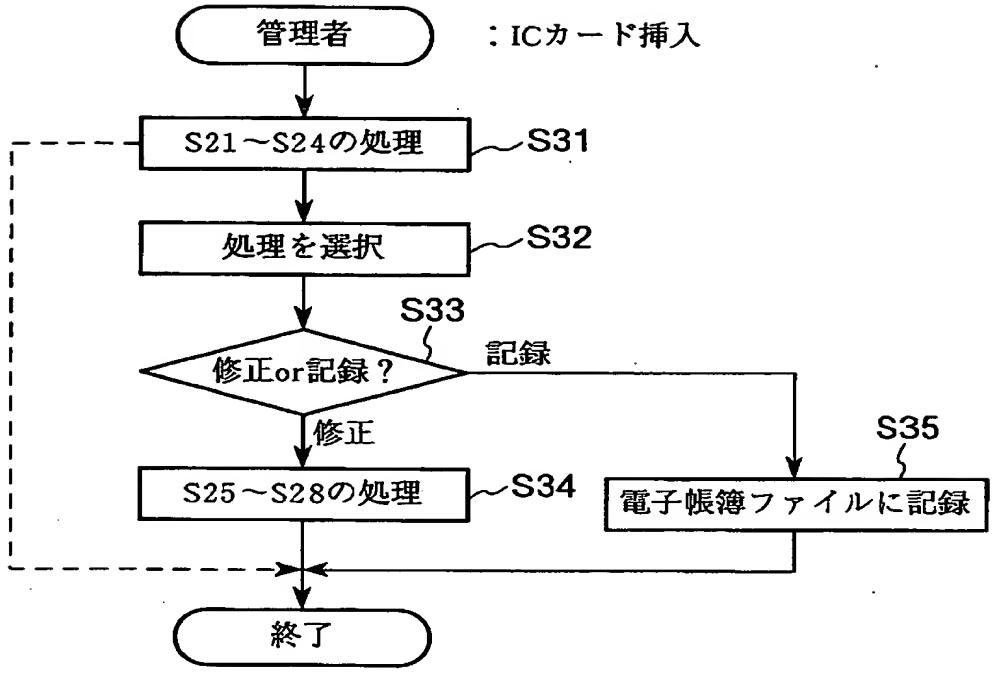
【図４】


ユーザー
：磁気カード挿入
取引情報に電子署名をして入力
S11
暗号化して履歴管理ファイルに記録
S12
電子帳簿ファイルに記録
S13
終了

【図５】

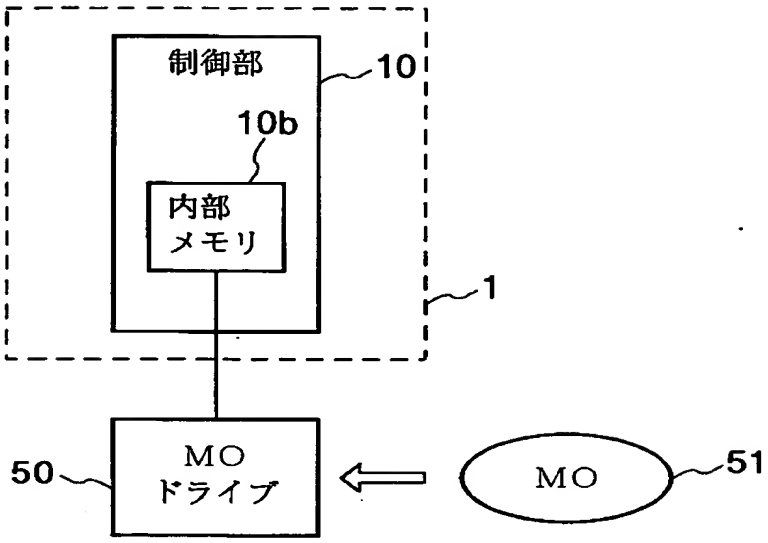

管理者
：ICカード挿入
チャレンジレスポンスで機器認証
S21
S22
OK？
NO
YES
指紋照合
S23
S24
一致？
NO
YES
履歴管理ファイルを復号化して出力
S25
修正データを入力
S26
暗号化して履歴管理ファイルに記録
S27
電子帳簿ファイルに記録
S28
終了

【図６】

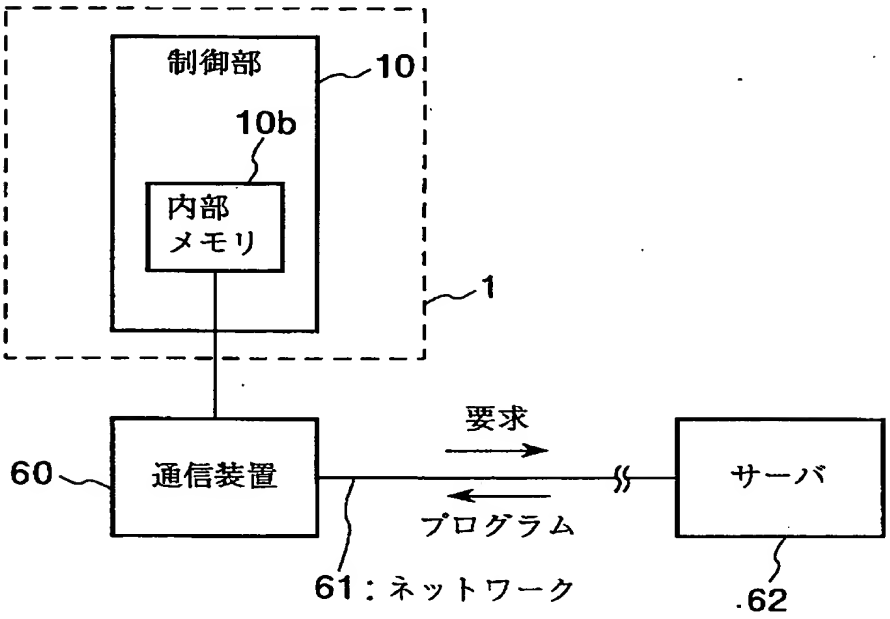

管理者
：ICカード挿入
S21～S24の処理
S31
処理を選択
S32
S33
修正or記録？
記録
修正
S35
S25～S28の処理
S34
電子帳簿ファイルに記録
終了

【図７】

(a)


制御部
10
10b
内部
メモリ
1
50
MO
ドライブ
MO
51

(b)


制御部
10
10b
内部
メモリ
1
60
通信装置
要求
プログラム
サーバ
61：ネットワーク
62

【書類名】　要約書

【要約】

【課題】　電子帳簿などの電子データの管理について、高いセキュリティを達成する。

【解決手段】　ユーザは、磁気カード２を磁気カードリーダ１１に読み取らせ、電子署名と共に取り引き情報を入力装置１８から入力する。この取り引き情報は、電子署名と共に電子帳簿ファイル１６に記録され、暗号化されて履歴管理ファイル１７に記録される。管理者は、取り引き情報を修正するとき、ＩＣカード４をＩＣカードリード／ライト１４に挿入してＳＡＭ１５との間で機器認証させると共に、指紋ファイル１３に記録された指紋のデータと当該管理者の指紋３のデータとを指紋認証装置１２に照合させる。機器認証、指紋の認証の双方が得られると、制御部１０は履歴管理ファイル１７を復号化し、電子帳簿ファイル１６の修正を可能とさせる。そして、管理者が入力した電子帳簿ファイル１６の修正に関するデータも暗号化されて履歴管理ファイル１７に記録される。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００１６８２８５〕

１．変更年月日　　１９９０年　８月　９日
［変更理由］　新規登録
住　所　　山梨県甲府市大津町１０８８－３
氏　名　　甲府日本電気株式会社